⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭61－16643

⑤1Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　昭和61年(1986)1月24日
H 04 L 9/02		Z－7240－5K	
H 04 K 1/00		Z－7240－5K	

審査請求　未請求　発明の数 1　（全9頁）

⑤4発明の名称　加入者キー再生システム

⑳特　願　昭60－48433

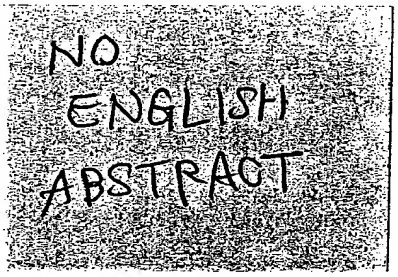
㉒出　願　昭60(1985)3月13日

優先権主張　㉜1984年3月15日㉝米国(US)㉛589741

⑦2発明者　カール・イー・モーグー　アメリカ合衆国，カリフオルニア州　92064，ポーウエイ，ホワイトウオーター・ドライブ　13360

⑦1出願人　エム／エーコム・リンカビツト・インコーポレーテツド　アメリカ合衆国，カリフオルニア州　92121，サンデイエゴ，サイエンス・パーク・ロード　3033

⑦4代理人　弁理士　鈴江　武彦　外2名



明　細　書

1. 発明の名称

加入者キー再生システム

2. 特許請求の範囲

(1)　ディスクランプラに固有であると共に、エンコードキー信号，キー生成ナンバーおよび上記ディスクランプラに含まれるメモリの所定の領域をアクセスするアドレスと共に上記ディスクランプラによって受信されるスクランブル信号のディスクランプリング用としてデコードすべきキー信号のエンコード時に使用される加入者キー信号を上記ディスクランプラで再生するシステムであって、

上記ディスクランプラに固有な加入者キー生成信号を供給する手段と、

上記ディスクランプラに固有な指定された加入者キーシード信号によってキーイングされるアルゴリズムに基く所定のエンコードアルゴリズムに従って上記加入者キー生成信号を処理することによって上記固有の加入者キー信号を再生する加入者キー生成器と、

上記指定された加入者キーシード信号を格納し、且つ上記指定されたシード信号を含む領域が上記キー生成ナンバーと共に受信される上記アドレスによってアクセスされたとき上記アルゴリズムをキーするために上記指定されたシード信号を供給する第1のメモリと、

上記キー生成ナンバーと共に受信される上記アドレスでもって上記第1のメモリをアクセスする手段とを具備してなる加入者キー再生システム。

(2)　上記第1のメモリが上記キー生成ナンバーと共に受信される上記アドレスに従って上記アルゴリズムをキーするために供給されている上記シード信号のうちの指定された一つを伴なう複数の異なる加入者キーシード信号を格納する特許請求の範囲第1項に記載の加入者キー再生システム。

(3)　上記加入者キー生成信号を供給する手段が上記ディスクランプラに固有な加入者アドレ

ス信号を格納する第2のメモリと、上記格納された加入者アドレス信号と上記加入者キー生成信号を供給するために受信される上記キー生成ナンバーとを結合させる手段とからなる特許請求の範囲第1項記載の加入者キー再生システム。

3.発明の詳細な説明

〔発明の技術分野〕

この発明は一般にエンコードテクノロジーに利用される通信信号スクランブリングおよびディスクランブリングシステムに係り、特にディスクランブラに固有であると共にディスクランブラによって受信された信号のディスクランブリング用としてデコードすべきキー信号のエンコーディング時に使用されているキー信号をディスクランブラで再生するシステムを志向している。

〔発明の技術的背景およびその問題点〕

従来、デコードすべきキー信号のエンコーディング時に使用される上記固有のキー信号はディスクランブラに含まれているメモリに格納されてしまうからである。

この問題に対する一つの解決は例えば、固有のディスクランブラの加入者キー信号を格納する各ディスクランブラに安全なメモリを使用するもので、上記米国特許出願№498,800によって示唆されている。安全なメモリは集積回路化マイクロプロセッサチップ中の内部的なリードオンリメモリ(ROM)であり、このチップはチップの読み取りからROMを予防する内部アーキテクチャを有しているものとする。この安全なメモリへのアプローチはかかるディスクランブラ用の固有な加入者キー信号を確認するディスクランブラの所有者に対して高レベルの安全性を与える。

〔発明の目的〕

この発明の目的は許可されない確認およびキー信号の使用の可能性をさらに少なくし得るようにディスクランブラにおける固有な加入者キー信号の再生を複雑にすることにある。

この発明の別の目的は個々の加入者および個々の放送者の双方に固有な加入者キー信号を使用して共通加入者通信ネットワークに有用とする複数の放送者にとって実際的な対処をなさしめる如く加入者キー信号の再生を複雑にすることにある。

〔発明の概要〕

この発明は、ディスクランブラに固有であると共にディスクランブラによって受信された信号のディスクランブリング用としてデコードすべきキー信号のエンコーディング時に使用されている加入者キー信号を加入者通信ネットワークのディスクランブラで再生するシステムである。

この発明によると、スクランブル信号はエンコードキー信号、キー生成ナンバーおよびディスクランブラに含まれるメモリの所定の領域をアクセスするアドレスと一緒にディスクランブラによって受信される。上記スクランブル信号が上記エンコードキー信号およびキー生成ナンバーと共に受信されるという言い方は必ずしも

これらの信号が一時的に一緒に受信されるということを意味するものでなく、むしろ全てがディスクランプラによって受信されるという方がよい。実際、一般的に所定のスクランブル信号のディスクランプリング用のエンコードキー信号は所定のスクランブル信号の送信および受信の前にディスクランプラに送信され且つ受信される。

この発明のシステムはディスクランプラに固有な加入者キー生成信号を供給する手段と、ディスクランプラに固有な指定された加入者キーシード信号によってキーイングされるアルゴリズムに基く所定のエンコードアルゴリズムに従って加入者キー生成信号を処理することによって固有の加入者キー信号を再生する加入者キー生成器と、指定された加入者キーシード信号を格納し且つ指定されたシード信号を含む領域がキー生成ナンバーと共に受信されるアドレスによってアクセスされたときアルゴリズムをキーするために指定されたシード信号を供給する第1のメモリと、キー生成ナンバーと共に受信されるアドレスでもって第1のメモリをアクセスする手段とを含んでいる。好ましくは第1のメモリは安全メモリである。

この発明のシステムは特に、複数の加入者のそれぞれに対して固有にエンコードされ、且つスクランプル信号のディスクランプリングに使用するために各加入者に固有な加入者キー信号の使用によってデコードすべき共通のキー信号をとる加入者通信ネットワークに有用である。

この発明のシステムはまた特に、複数の異なるスクランプル信号放送者によって加入者に対し固有にエンコードされ、且つスクランプル信号のディスクランプリングに使用するために加入者および放送者の双方に固有な加入者キー信号を使用することによってデコードすべき共通のキー信号をとる加入者通信ネットワークに有用であり、ここで加入者は固有にエンコードされたキー信号をデコードするために所定の放送者に固有な加入者キー信号を使用することによって所定の放送者からのスクランプル信号を個別的にディスクランプリングするディスクランプラを有している。

好ましくは上記第1のメモリは、キー生成ナンバーと共に受信されるアドレスに従ってアルゴリズムをキーするために供給されている上記シード信号のうちの指定された一つを伴なう複数の異なる加入者キーシード信号を格納する。所定の放送者によって使用されている現行の加入者キー信号のリストが知られた事実となったら、放送者はキー生成ナンバーを変更するかまたは加入者ネットワークの各ディスクランプラの第1メモリから異なる加入者キーシード信号をアクセスするアドレスを変更すればよく、その結果として加入者キー信号の完全に異なるリストがネットワークに適用可能とし得る。

システムをさらに複雑にするには、ディスクランプラ内で加入者キー生成信号を供給する手段の好ましい実施例が、ディスクランプラに固有な加入者アドレス信号を格納する第2のメモリと、上記格納された加入者アドレス信号と上記加入者キー生成信号とを結合する回路とを含んでいればよい。

このテクニックは共通加入者通信ネットワークを利用する異なる放送者に対して固有なキー生成ナンバーを可能とするので、異なる固有の加入者キー信号が異なる放送者によって送出されるスクランプル信号を各別にディスクランプリングする使用のために所定のディスクランプラで再生される。また、各放送者は共通グループの加入者に対して共通キー生成ナンバーを送出することを可能とする。

〔発明の実施例〕

先ず、この発明の前提となる上述した米国特許出願№498,800に開示された内容について説明すると、全体的なスクランプリングおよびディスクランプリングのうちのスクランプリング部分において、テレビジョン信号はスクランプラキー分配システムによって生成されるキーストリームでもって映像および音声部分を処理す

ることによってスクランブルされる。このスクランブラキー分配システムはコントロールコンピュータによって供給されるチャンネルキー信号によってキーイングされたアルゴリズムに基くデータエンコードスタンダード(DES)アルゴリズムによってキーストリームを生成する。チャンネルキー信号はテレビジョン信号をディスクランブルするディスクランブラに必要となる。このテレビジョン信号の許可されないディスクランブリングを防止するために、チャンネルキー信号はスクランブルテレビジョン信号をスクランブルすることを許可された加入者のグループに共通のカテゴリキー信号によってキーイングされたアルゴリズムに基くDESアルゴリズムによってエンコードされる。エンコードされたチャンネルキー信号はスクランブル信号プロセッサによってスクランブルテレビジョン信号に挿入された後、加入者ネットワークのディスクランブラに送出される。

上記カテゴリキー信号もまたエンコードされることになるが、このカテゴリキーは加入者ネットワークの異なるディスクランブラにそれぞれ固有な加入者キー信号の各グループによってキーイングされるアルゴリズムに基いたDESアルゴリズムによって固有にエンコードされる。この固有にエンコードされたカテゴリキー信号はそれぞれのディスクランブラにアドレスされると共に、加入者ネットワークのそれぞれのディスクランブラにそれを送出するスクランブル信号プロセッサによってスクランブルテレビジョン信号に挿入される。

上記固有な加入者キー信号のリステングは加入者キー分配システムによる場合を除いては利用されないように維持される。このリステングが不許可のアクセスによって危険にさらされたら、加入者キー信号の新しいリステングが準備され且つ利用されなければならない。上記コントロールコンピュータはまた放送者に固有なシステムキー生成ナンバーをスクランブラ信号プロセッサに供給し、このシステムキー生成ナンバーはまた全ての加入者への送信用としてスクランブルテレビジョン信号中に挿入される。さらにスクランブラ信号処理器はスクランブルテレビジョン信号中にコントロールコンピュータによって供給されたプロセスコントロール信号および初期化ベクトル(IV)フレームカウント信号を挿入する。

上記スクランブルテレビジョン信号をディスクランブルするために各ディスクランブラにおいては、テレビジョン信号をスクラン(ブル)するのに使用されたキーストリームが再生されなければならない。ディスクランブラでキーストリームを再生するためには、エンコードチャンネルキー信号がスクランブラのキーストリームを生成するのに使用されたチャンネルキーを再生するためにデコードされなければならない。所定のディスクランブラにおけるエンコードチャンネルキー信号をデコードするためには、所定のディスクランブラに対してアドレスされた固有のエンコードカテゴリキーがスクランブラにおいてチャンネルキー信号をエンコードするのに使用されたカテゴリキー信号を再生するのにデコードされなければならない。所定のディスクランブラにおける固有のエンコードカテゴリキー信号をデコードするためには、スクランブラにおいてカテゴリキー信号をエンコードするのに使用された固有の加入者キー信号がそのディスクランブラにおいて再生されなければならない。

第1図を参照すると、ディスクランブラはディスクランブラ信号プロセッサ150およびディスクランブラキー分配システム151とを含んでいる。

このディスクランブラ信号プロセッサ150はライン152のスクランブルテレビジョン信号を受信する。ディスクランブラ信号プロセッサ150は上記受信したスクランブルテレビジョン信号からディスクランブラキー分配システム151の動作に関係するIVフレームカウント信号(図示せず)エンコードチャンネルおよびエンコードカテゴリキー信号(ライン156)、加入

者キー生成ナンバー（ライン157）および種々のプロセスコントロール信号（ライン158）を分離してディスクランブラーキー分配システム151に供給する。

このディスクランブラキー分配システム151はライン162で受信したスクランブルテレビジョン信号の映像および音声成分をスクランブルするのに使用された固有のキーストリームを再生することによって信号プロセッサからライン156～158を介して受信されたそれらの信号に応答し、ライン159を介してディスクランブラ信号プロセッサ150に固有のキーストリームを供給する。

ディスクランブラ信号プロセッサ150はライン160にディスクランブルされた映像信号を且つライン161にディスクランブルされた音声信号を供給するために、ライン159で受信された固有のキーストリームに従ってライン152のスクランブルテレビジョン信号をディスクランブルする。

第2図を参照すると、第1図のディスクランブラキー分配システムシステム151において使用される加入者キー再生システムの一つの好ましい実施例は、4つの加入者キーシード信号を格納する安全な加入者キーシードメモリ163と、ディスクランブラに固有な加入者アドレス信号を格納する加入者アドレスメモリ164と、加入者キー信号生成器165とを含んでいる。

上記メモリ163は格納されている4つの固有な加入者キーシード56ビット信号をライン179に供給するために、ライン157で受信された32ビットシステムキー生成ナンバーの所定の位置に含まれている2ビットによりライン298を介してアドレスされる。

メモリ164に格納されている32ビットの固有な加入者アドレス信号は、ライン180に64ビットの加入者キー生成信号を供給するために、ライン157で受信された32ビットシステムキー生成ナンバーと結合される。

加入者キー生成器165は、ライン179の固有な加入者キーシード信号によってキーイングされたDESアルゴリズムによるDESエンコードアルゴリズムに従ってライン180の加入者キー生成信号を処理することにより、ライン181に固有な64ビットの加入者キー信号を生成する。ライン181の固有な加入者キー信号のうちの8ビットは、ディスクランブラにアドレスされた固有なエンコードカテゴリキー信号の生成をキーするのにスクランブラにおいて使用されている固有な56ビット加入者キー信号を再生するために切り捨て機能素子166によって取り除かれる。

安全メモリ163からライン179に引き出された加入者キーシード信号の内容に基いて加入者キー生成器165によりライン181に生成された加入者キー信号の内容が重要である故に、ディスクランブラにアドレスされた固有のエンコードカテゴリキー信号の生成をキーするのにスクランブラにおいて使用されたそれと全く同一の固有な加入者キー信号の生成をキーすることになる加入者キーシード信号に含まれている安全メモリ163のロケーションをシステムキー生成ナンバーにおける2つのアドレスビットがアドレスする。

ディスクランブラキー分配システム151はさらにカテゴリキー生成器167を含んでいる。このカテゴリキー生成器167はライン156にアドレスされた固有なエンコードカテゴリ信号を受信し、そしてライン182に固有の加入者キー信号が再生されたとき、ライン182の固有な加入者キー信号によってキーイングされたDESアルゴリズムに基くDESエンコードアルゴリズムに従ってライン156を介して受信されたエンコードカテゴリキー信号を処理することにより、ライン183にデコードされた64ビットのカテゴリキー信号を生成する。

図示しないキーストリーム生成器を除いて、第1図のディスクランブラキー分配システム151の構成要素は全てシングルマイクロプロセッサチップに含まれるものとし、具体的には

例えばインテル社製8751シングルコンポーネント8ビットマイクロコンピュータのスペシャルバージョンでよい。インテル社製8751に代るものとしては同一性能を与えるテキサスインスツルメンツ社製TMS7041とTMS70C40との組合せがある。インテル社製"8751"チップはHMOSテクノロジーで製作されたスタンドアロン，ハイパフォーマンス，シングルチップのコンピュータであって、40ピンDIPにパッケージされている。それはこの種の暗号法の応用における効果的なコントローラとして必要なハードウエア上の特徴、アーキテクチュラルエンハンスメントおよびインストラクションセットを提供する。このスペシャルバージョンの8751チップのEPROMはチップに読み出すのみの4Kバイトの UV消去リードオンリメモリを含んでいる。アーキテクチュアは製造プロセスにおいて"ベリファイモード"のヒューズをとばすことによって外部ベリファイモードが不能になされているならば、EPROMからチップの外側に向う通路をいささかとも提供しない。全てのファームウエアはこのEPROM領域に含まれるキー信号の生成およびストレージを遂行する。8751チップの安全なEPROMに格納されたプログラムを読み出すことの極度の困難さは加入者キー信号および加入者アドレスのリストの使用をなすための剽窃にとってはるかに多くの困難をもたらす。これは、たとえ剽窃者がそのリストを得るのにコントロールコンピュータの安全システムの破壊に成功したとしてもである。若し、剽窃者が確かな加入者キー信号を知っていたとしても、その者はその者がメモリ中に確かな加入者キー信号シードおよび加入者アドレスを格納し得る全体のプログラムを知らなければならない。これは製造者のセキュリティ手続きによって保護される完全なプログラムリストなしでするのは極めて困難である。

第3図および第4図に示される好ましい実施例における固有な加入者キー信号の再生は2つの異なるキーシード信号を実用化することによってさらに複雑となっている。

第3図の実施例は加入者キーシードメモリ163，加入者アドレスメモリ164および第2図の実施例に含まれている加入者キー生成器165を含むと共に、さらに第2のキー生成器300を含んでいる。

メモリ163は、格納された4つの固有な加入者の56ビットキーシード信号の第1指定部をライン179に供給するために、ライン157で受信された32ビットのシステムキー生成ナンバーの第1の所定位置に含まれている2ビットによってライン298を介してアドレスされると共に、格納された4つの固有な加入者キーシード信号の異なる第2指定部をライン301に供給するために、ライン157で受信されたシステムキー生成ナンバーの第2の所定位置に含まれている2ビットによってさらにアドレスされる。

メモリ164に格納されている32ビットの固有な加入者アドレス信号は、ライン302に64ビットの第2のキー生成信号を供給するためにライン157で受信された32ビットの加入者キー生成ナンバーに結合される。

第2のキー生成器300は、ライン301の第2指定部の固有な加入者キーシード信号によってキーイングされるDESアルゴリズムに基くDEPエンコードアルゴリズムに従ってライン302の第2のキー生成信号を処理することによってライン303に64ビットの固有な加入者キー生成信号を生成する。

加入者キー生成器165は、ライン179の第1指定部の固有な加入者キーシード信号によってキーイングされるDESアルゴリズムに基くDESエンコードアルゴリズムに従ってライン303の加入者キー生成信号を処理することによってライン181に64ビットの固有な加入者キー信号を生成する。ライン181の固有な加入者キー信号のうちの8ビットはディスクランプラにアドレスされた固有なエンコードカテゴリキー信号の生成をキーするのにスクランプ

ラにおいて使用されている固有な加入者キー信号と全く同一の固有な５６ビットの加入者キー信号をライン１８２に供給するために切り捨て機能素子１６６によって取り除かれる。第３図のシステムのこの他の全ての態様は第２図のシステムと同じである。

第４図の実施例は加入者キーシードメモリ１６３，加入者アドレスメモリ１６４，加入者キー生成器１６５および第３図の実施例に含まれている第２のキー生成器３００を含むと共に、さらに第３のキー生成器３０５を含んでいる。

メモリ１６３は、格納されている４つの固有な加入者５６ビットキーシード信号の第１指定部をライン１７９に供給するのに、ライン157で受信された３２ビットのシステムキー生成ナンバーの第１の所定位置に含まれる２ビットによってライン２９８を介してアドレスされると共に、さらに格納されている４つの固有な加入者キーシード信号のうちの異なる第２指定部をライン３０１に供給するのに、ライン１５７で受信されたシステムキー生成ナンバーの第２の所定位置に含まれる２ビットによってアドレスされる。

メモリ１６４に格納されている３２ビットの固有な加入者アドレス信号は、ライン３０６に６４ビットの第３のキー生成信号を供給するのにライン１５７で受信された３２ビットの加入者キー生成ナンバーと結合される。

第３のキー生成器３０５は、ライン１７９の第１指定部の固有な加入者キーシード信号によってキーイングされるDESアルゴリズムに基くDESエンコードアルゴリズムに従ってライン３０６の第３のキー生成信号を処理することによってライン３０７に６４ビットの固有な第２のキー生成信号を生成する。

第２のキー生成器３００は、ライン３０１の第２指定部の固有な加入者キーシード信号をDESアルゴリズムに基くDESエンコードアルゴリズムに従ってライン３０７の第２のキー生成信号を処理することによってライン３０３に６４ビットの固有な加入者キー信号を生成する。

加入者キー生成器１６５は、ライン１７９の第１指定部の固有な加入者キーシード信号によってキーイングされるDESアルゴリズムに基くDESエンコードアルゴリズムに従ってライン３０３の加入者キー生成信号を処理することによってライン１８１に６４ビットの固有な加入者キー信号を生成する。ライン１８１の固有な加入者キー信号のうちの８ビットはディスクランプラにアドレスされた固有なエンコードカテゴリキー信号の生成をキーするのにスクランプラにおいて使用されている固有な加入者キー信号と全く同一の固有な５６ビットの加入者キー信号をライン１８２に供給するために切り捨て機能素子１６６によって取り除かれている。第４図のシステムのこの他の態様は第２図のシステムと同じである。

〔発明の効果〕

上述したところから明らかであるように、この発明の加入者キー再生システムは多くの有利な特徴を有している。

１つの特徴は再生される固有な加入者キー信号をスクランプラのコントロールコンピュータによって供給されると共にディスクランプラに送出するためのスクランプルド信号に挿入されるシステムキー生成ナンバーを変更することによって簡単に変更することができるということである。

別の特徴は所定の加入者通信ネットワーク用の固有な加入者キー信号の異なるセットは異なる放送者による使用のために生成することができるということであり、これによって異なる放送者からのスクランプルド信号は同じディスクランプラによって固別的にディスクランプルすることができる。従って、このシステムを使用する各放送者は他の放送者のリスティングの機密性を危険にさらすことなく、固有の加入者キー信号そのものの独立したリスティングを準備することができる。

付加的な特徴は、ディスクランプラのメモリ

中の複数の異なるキーシード信号の蓄積が、ストリームキー生成ナンバーの共通アドレスによってアクセスされるキーシード信号の1つのリスティングが危険にさらされるという事態の支援を準備するということである。

さらなる特徴は、加入者ネットワークの固有の加入者キー信号の新しいリスティングを生成するときに、共通にアドレスされるキーシード信号のリスティングのうちの必要な一つのみが機密ストレージより取り除かれるということであり、これによってかかる生成処理中に全てのネットワークの安全性を危険にさらすことの可能性が減少する。

この発明のシステムの好ましい実施例はここでは加入者テレビジョンネットワークに使用する場合について述べたが、この発明のシステムは例えば加入者電話ネットワークのような他のタイプの加入者通信ネットワークに有用であり且つ適用可能である。加入者電話ネットワークでは、各加入者は本質において放送者であると共に、スクランブラとディスクランブラの両方を所有している。従って、各加入者はそのネットワークの他の加入者のディスクランブラに送出するのを可能とする固有の加入者キーナンバーそのものの固有なリスティングを準備し得ると共に、そのネットワークの他の全ての加入者に共通に送出する相関されたシステムキー生成ナンバーを準備し得る。固有の加入者キー信号のうちのある加入者のリスティングが危険にさらされたとしても、他の加入者のリスティングは同じように危険にさらされることがないと共に、ある加入者は簡単に新しいリスティングおよび新しく相関されたシステムキー生成ナンバーを準備することができる。

この発明のシステムはそのうえ上述した加入者電話ネットワークと同様にして加入者コンピュータインターフェイスネットワークにも有用である。

4. 図面の簡単な説明

第1図はこの発明のシステムに有用なディスクランブラの機能的なブロックダイアグラムであり、

第2図はこの発明の加入者キー再生システムの一つの好ましい実施例の機能的なブロックダイアグラムであり、

第3図はこの発明の加入者キー再生システムの別の好ましい実施例の機能的なブロックダイアグラムであり、

第4図はこの発明の加入者キー再生システムのさらに別の好ましい実施例の機能的なブロックダイアグラムである。

150…ディスクランブラ信号プロセッサ、*151*…ディスクランブラキー分配システム、*163*…加入者キーシードメモリ、*164*…加入者アドレスメモリ、*165*…加入者キー信号生成器、*166*…切り捨て機能素子、*167*…カテゴリキー生成器。

FIG. 1

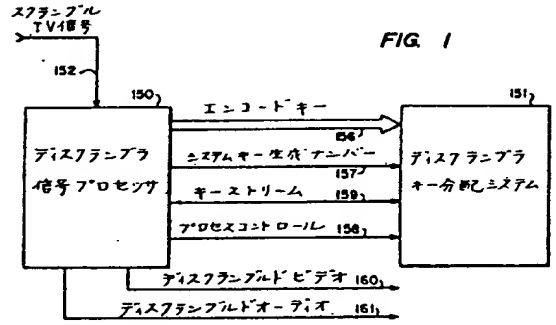
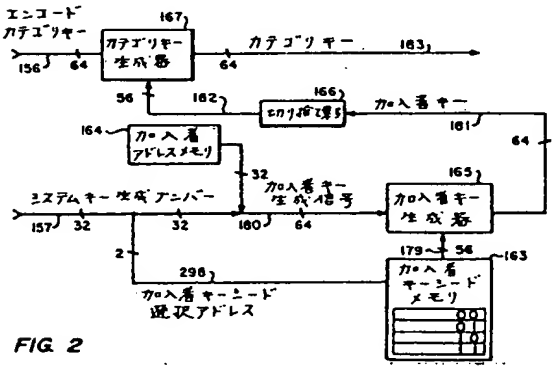


FIG. 2



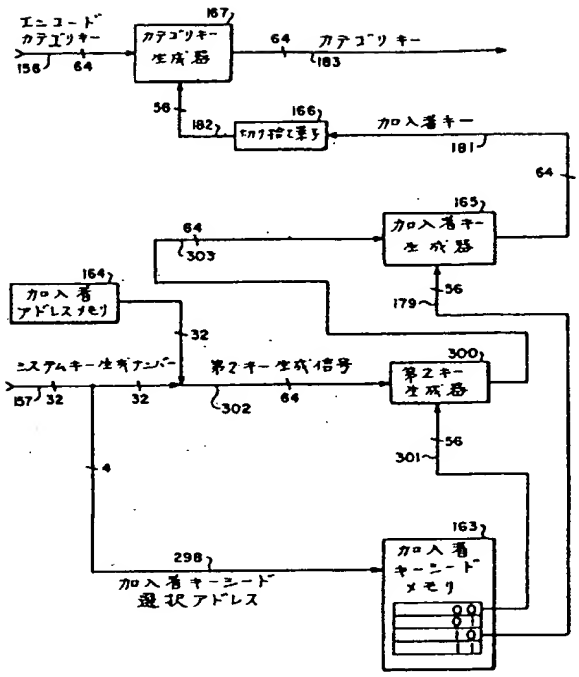

エニコード
カテゴリキー
156
64
167
カテゴリキー
生成器
64
カテゴリキー
183
56
182
166
切り捨て手段
加入者キー
181
64
165
加入者キー
生成器
64
303
56
179
164
加入者
アドレスメモリ
32
システムキー生成ナンバー
157
32
第2キー生成信号
32
302
64
300
第2キー
生成器
56
301
4
298
163
加入者
キーコード
メモリ
加入者キーコード
選択アドレス

FIG. 3

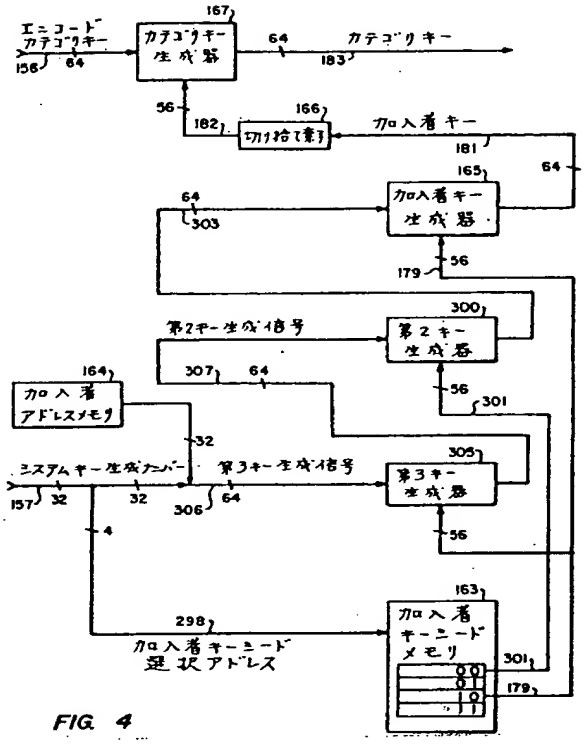

エニコード
カテゴリキー
156
64
167
カテゴリキー
生成器
64
カテゴリキー
183
56
182
166
切り捨て手段
加入者キー
181
64
165
加入者キー
生成器
64
303
56
179
第2キー生成信号
300
第2キー
生成器
307
64
56
301
164
加入者
アドレスメモリ
32
システムキー生成ナンバー
157
32
第3キー生成信号
32
306
64
305
第3キー
生成器
56
4
298
163
加入者
キーコード
メモリ
301
179
加入者キーコード
選択アドレス

FIG. 4